Содержание

1. Лабораторная работа № 1. Исследование зависимости криптостойкости от длины ключа

1.1. Информация по стенду

- Требуемые ВМ
  - **deb10-1**
- Вход в систему

```
sysadmin:netlab123
```

- Получение привилегий суперпользователя (пароль netlab123)

```
$ su -
```

1.2. Утилита fcrackzip

fcrackzip - утилита для восстановления/взлома паролей zip-архивов

Может использоваться и как инструмент восстановления данных и как инструмент злоумышленника

1.3. Подготовка системы

Задание выполняется на ВМ **deb10-1**, потребуется подключение к сети Internet.

- Установка необходимых компонент в ОС Debian (выполняется под УЗ суперпользователя)

```
$ apt update && apt install fcrackzip zip unzip git
```

Убедитесь, что компоненты установлены.

- Получение файлов, необходимых для выполнения лабораторной работы. Выполняется на ВМ, войдя в систему под УЗ **sysadmin** и находясь в его домашнем каталоге

```
$ git clone https://github.com/esorlov/infsec/
```

- Перейдите в каталог текущей лабораторной работы

```
$ cd infsec/lab1
```

- Убедитесь, что присутствуют файл **opentext.txt** и скрипт создания отчета по лабораторной работе **report**

```
$ pwd
/home/sysadmin/infsec/lab1
$ ls
opentext.txt  report
```

1.4. Задание 1. Создание зашифрованных zip-архивов

Создание зашифрованных ZIP-архивов производится командой

```
$ zip -e <archive.zip> <files...>
```

Пароль для создания ключа шифрования вводится с клавиатуры

- Выполните создание из файла **opentext.txt** зашифрованных архивов в соответствии со следующей таблицей.

Имя архива	содержимое	длина пароля	пароль
archive2.zip	opentext.txt	2	ne
archive3.zip	opentext.txt	3	net
archive4.zip	opentext.txt	4	netl
archive5.zip	opentext.txt	5	netla
archive6.zip	opentext.txt	6	netlab

- Пример

```
$ zip -e archive2.zip opentext.txt
. . .
$ zip -e archive3.zip opentext.txt
. . .
```

- Попробуйте открыть один из архивов при помощи **неверного пароля**. Убедитесь, что это невозможно.
- Убедитесь, что при указании **верного пароля** от архива возникает предложение перезаписать уже существующий в текущем каталоге файл **opentext.txt**. Т.е. извлечение файла становится возможным.

1.5. Восстановление паролей зашифрованных ZIP-архивов

В этой части задания якобы потерянные пароли от зашифрованных ZIP-архивов будут восстановлены с использованием специальной утилиты **fcrackzip**.

Fcrackzip пытается восстановить пароль архива методом полного перебора (метод грубой силы).

Ваша задача понять как длина указанного при создании архива пароля, т.е. по сути длина ключа шифрования влияет на время необходимое на осуществление полного перебора (выполнение атаки на криптосистему методом грубой силы).

- Ознакомьтесь со справкой по команде **fcrackzip**

```
$ fcrackzip -h
```

Для восстановления пароля мы будем использовать следующее сочетание опций

```
-vul min-max -c a
```

где -l min-max - диапазон длины пароля от минимального до максимального значения, -v - подробно -u - использовать unzip -c a - перебирать среди символов нижнего регистра

- Попробуйте восстановить пароль, например для архива **archive3.zip**, используя следующую команду

```
$ fcrackzip -vul 3-3 -c a archive3.zip
```

Соответствует ли восстановленный пароль ранее введенному?

1.6. Задание 2. Исследование времени восстановления паролей

Для определения точного времени, необходимого на восстановление пароля от зашифрованного архива мы будем использовать утилиту **time**

- Выполните следующие команды и зафиксируйте время их выполнения по выводу утилиты **time** (
- Интересует общее время, т.е. значение в строчке **real**

```
$ time fcrackzip -vul 2-2 -c a archive2.zip
$ time fcrackzip -vul 3-3 -c a archive3.zip
$ time fcrackzip -vul 4-4 -c a archive4.zip
$ time fcrackzip -vul 5-5 -c a archive5.zip
$ time fcrackzip -vul 6-6 -c a archive6.zip
```

Если требуемое для перебора время превышает несколько минут, например при восстановлении archive6.zip, продолжать не стоит, достаточно результата полученного для длины 5 символов.

- Выполните указанные выше команды по 3 раза, чтобы иметь возможность усреднить значение времени перебора. Полученные значения времени T1, T2 и T3 для каждого значения длины пароля зафиксируйте в таблице вида

K, Длина пароля	T1, Время, мс	T2, Время, мс	T3, Время, мс	T, Среднее время, мс
2				
3				
4				
5				
6				
7				
8				

1.7. Задание 3. Подсчет скорости перебора паролей

Сложность перебора (C) оценивается как мощность алфавита (N) возведенной в степень длины пароля (K)

$$C = N^K$$

Скорость перебора S - это сложность перебора (C), разделить на время (T)

$$S = \frac{C}{T} = \frac{N^K}{T}$$

- Исходя из полученных в предыдущем пункте данных о времени выполнения восстановления пароля оцените приблизительную скорость перебора в **символах в миллисекунду**, выполнив подсчет для различных длин пароля. используйте калькулятор. Мощность алфавита - 26 (символы нижнего регистра, англ).

  При получении в результатах времени, большего, чем 1 минута, необходимо правильно выполнить преобразование в секунды/милисекунды, например

```
$ time fcrackzip -vul 6-6 -c a archive6.zip
found file 'opentext.txt', (size cp/uc    278/   447, flags 9, chk 4e09)
checking pw ndjtfz

PASSWORD FOUND!!!!: pw == netlab

real    17m7,197s
user    14m57,000s
sys 1m57,980s
```

Время - 17 минут 7,197 секунд

```
17*60 + 7,197 = 1027,197
```

- Для фиксации результатов можно использовать следующую таблицу. Для длин от 2 до 5(6) среднее время должно быть измерено в Задании 2, а скорость вычислена. Для длин больших 5(6) необходимо оценить предполагаемое время на основании оценочной скорости перебора.

K, Длина пароля	T, Среднее время, мс	S, Скорость перебора
2		
3		
4		
5		
6		
7		
8		

  Обратите внимание, что скорость перебора должна возрастать по мере увеличения сложности, связано это с тем, что чем выше сложность тем меньше в полученном результате накладных расходов, связанных с выполнением вспомогательного кода, выполнением системных вызовов, ввода-вывода и т.п. В качестве оценочного значения скорости перебора возьмите значение полученное при использовании максимальной длины пароля. При необходимости выполните повторную оценку и скорректируйте данные.

- Используя полученную оценочную скорость перебора (S), оцените предполагаемое время в миллисекундах-секундах-минутах-часах, необходимое для перебора пароля длиной 7 и 8 символов

$$T = \frac{N^K}{S}$$

- Попробуйте изменить мощность словаря, используемого при переборе, убрав ограничение на перебор только по буквам нижнего регистра

```
$ time fcrackzip -vul 4-4 archive4.zip
```

  Оцените, как в этом случае поменялось время перебора

- **Внимание!** Стоит учесть, что время восстановление ключа не позволяет точно определить скорость перебора, т.к. не перебираются все возможные комбинации, а столько сколько встречается до нахождения совпадения. Тем не менее, полученные в лабораторной значения позволяют оценить изменение сложности перебора в зависимости от длины ключа.

1.8. Задание 4. Отчет по лабораторной

- Запустите скрипт **report** из каталога текущей лабораторной

```
$ sh report
```

- Укажите свои ФИО, номер группы и ответьте на вопросы исходя из полученных вами данных.
- Полученный в итоге работы скрипта файл с закодированным содержимым - это ваш отчет по лабораторной. Его (только файл) необходимо загрузить в moodle в качестве отчета по лабораторной работе.